APHIS INFORMATION VALUATION

1. PURPOSE

a. This Directive establishes policy and procedures for establishing relative values for information assets used in APHIS operations. This is fundamental to establishing an effective and cost efficient information systems security (ISS) program that operates on a risk management basis.

b. The fundamental purpose of any security measure is to prevent losses. The APHIS ISS program exists to prevent or mitigate loss, damage, or disruption of information resources, which have become essential to the delivery of services and Agency operations.

2. AUTHORITIES/REFERENCES

Foundation of the APHIS ISS program is contained in Directive 3140. 1., dated 9/15/99. Applicable national policy requirements regarding ISS are stated primarily in Presidential Decision Directive 63, Critical Infrastructure Protection; the Computer Security Act of 1987 (Public Law (P.L.) 100-235); the Computer Fraud and Abuse Act (I 8 U.S.C. See. 1030 [1993]); Office of Management and Budget (OMB) Circular No. A- 1 23, Management Accountability and Control; Appendix III of OMB Circular No. A- 1 3 0, Management of Federal Information Resources; Office of Management and Budget (OMB) Bulletin 90-08; and the Computer Fraud and Abuse Act (I 8 U. S.C. Sec. 1030 [1993]). Taken together, these documents and others not cited prescribe the requirement to establish and maintain a comprehensive ISS program and set standards for use of information systems, including Intemet connections and usage. Additionally, United States Department of Agriculture (USDA), Office of Information Resources Management (OIRM), Department Regulation 3140-1, USDA IRM Security Policy, applies, as do other appropriate USDA ISS policies as well as Federal requirements related to protecting sensitive information, such as the Privacy Act of 1974 (P.L. 93579, 5 U.S.C. 552a).

3. SCOPE

a. This Directive applies to:

(1) All APHIS employees and contractors.

(2) Other Federal agencies, State and local governments, and private organizations or individuals who use APHIS information systems to accomplish an APHIS business function.

All of the aforementioned are considered users and are included wherever the words "user" or "users" are referenced within this Directive.

b. APHIS information systems covered by this Directive include all computer hardware, software, and telecommunications that directly support APHIS business functions.

4. POLICY

a. The APHIS ISS program is established and operated on the basis of value of information assets. The value structure established by this Directive will be applied across the Agency, to promote consistent and cost-efficient safeguards.

(1) Existing application systems will use this value structure to determine the application's overall level of risk and identify needed safeguards.

(2) New applications will, as an initial step, use this value structure to determine the sensitivity of the application. Appropriate safeguards then will be developed as integral components of the application.

(3) General Support Systems (GSS) that form the backbone Information Technology infrastructure will be designed to provide the bulk of needed safeguards for "low" value information.

b. Safeguards will based on established information values and with careful consideration of:

(1) Current technological threats and available safeguards.

(2) Federal policies and recommendations.

(3) Generally accepted standards and practices throughout both Government and private sector operations.

5. RESPONSIBILITIES

a. The Chief Information Officer (CIO), Information Technology community (ITc) will:

(1) Provide general oversight for the APHIS ISS program, ensuring that goals are set and achieved to maintain credible and effective protection for the Agency's information assets.

(2) Appoint an Information Systems Security Program Manager (ISSPM) to manage the ISS program on behalf of the Administrator and provide the ISSPM with adequate resources to ensure implementation of established ISS requirements.

(3) Empower the ISSPM to lead and assist APHIS Program/Business Units in information systems security program development, including information valuation and risk assessment.

(4) Approve a minimum level of protection for GSS that is adequate to protect information valued at the "low" level, as defined by this Directive. This will ensure that all systems are protected with at least a baseline of security controls.

b. Deputy Directors of Program Units and heads of major business offices will:

(1) Be personally responsible for ensuring an effective ISS program in their organization, as mandated by references cited in section 2. above. They will provide for the integrity, availability, and confidentiality of information that is critical to meeting APHIS missions.

(2) Establish or approve the value for each major application within their area of responsibility. A major application is defined as "use of information and information technology to satisfy a specific set of user requirements that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to modification of the information."

(3) Appoint an Information Systems Security Manager (ISSM) to represent them on ISS matters and to implement the APHIS ISS program within their area of responsibility.

(4) Ensure that each major application is assigned a management official knowledgeable in the nature of the information and process supported by the application including management, personnel, operational, and technical controls used to protect it. Assigned management officials will assess risk associated with applications and will work closely with ISSM's and ISS Officers (ISSO's) to ensure an effective ISS program.

(5) Ensure that the results of identifying applications as "high..... moderate," or "low" value becomes the basis of identifying risks and establishing safeguards.

(6) Provide the necessary resources to ensure implementation of APHIS ISS policy and ensure that security is adequate for the value level of the application system and included in all stages of each application system's life cycle.

c. The ISSPM will:

(1) Be the lead ISS specialist for APHIS, managing the Agency's ISS program in a manner consistent with USDA and Federal policies, and serving as the Agency's authority on these issues.

(2) Develop and distribute a risk assessment tool based upon the information valuation criteria set forth in this Directive. Use of that tool will not be mandated (alternative methods of risk assessment are allowed) but will be encouraged to promote standardization of safeguards throughout APHIS.

(3) Monitor risk assessment processes throughout the Agency and ensure the inclusion of such assessments in system security plans.

(4) Lead in establishing a minimum level of protection for GSS that is adequate to protect information valued at the "low" level, as defined by this Directive.

(5) Advise management on methods to better ensure data and system confidentiality, integrity, and availability.

d. ISSM's for Program/Business Units will:

(1) Be the lead ISS specialist for their Unit, managing ISS efforts and serving as the Unit's authority on data valuation and risk assessment methods. (However, ISSM's are not the ones who decide on the value of information resources; that is a functional management responsibility.)

(2) Monitor the completion of system risk assessments and their inclusion in

application system security plans.

(3) Advise management on methods to better ensure data and system confidentiality, integrity, and availability.

6. IDENTIFYING THE VALUE OF MAJOR APPLICATION SYSTEMS

a. Identifying assets that need protection and determining how much protection is warranted is fundamental to any security program. Without a method to accomplish that, protective measures are likely to be ineffective, inconsistent, and not cost effective.

b. Efforts to quantify the value of Government information assets typically have consumed many resources without providing measurable improvements in security. Therefore, APHIS will adopt a more workable scheme by establishing "high," "medium," and "low" value categories. Those levels will be subdivided to identify the reason for establishing that value as well as confidentiality, integrity, or availability. **(NOTE:** This is not an attempt to place a value on APHIS information technology. The value of the data is of concern; not the fact that the data is in electronic form. The data could exist solely in paper form and still have the much the same value in terms of confidentiality, integrity, and availability. Our increasing reliance on IT systems, however, is a key driving force behind this endeavor.)

(1) Information availability is defined as the need for data to be protected from actions or events that would prevent it from being in the right place, at the right time, and in the form needed by the user. "If the data in my system became unavailable, or the processing and communication of the data became unavailable (excluding the APHIS network), the likely result would be..."

(2) Information confidentiality is the need for data to be protected from access or disclosure to persons or processes which have no legitimate need, right, or authorization to that information. "If the data in my system were disclosed to unauthorized persons, the likely result would be..."

(3) Information integrity is the need for data to be accurate, complete, and authentic; the requirement that information be protected from actions that would preclude it from remaining a true and complete representation of its original content. "If the data in my system became inaccurate or incomplete to a significant degree, the likely result would be..."

c. The value structure model described can be illustrated with a matrix:

	Confidentiality	Integrity	Availability
High Value			
Medium Value			
Low Value			

d. The following criteria will be used to determine where application systems fit in the above matrix.

(1) Information Confidentiality.

(a) High value: If the information were disclosed to unauthorized persons, the likely result would be one or more of the following:

1 Danger to human life.

2 Grave threat to American food supplies or APHIS' ability to protect American food supplies and/or support American agriculture and export markets.

3 A monetary loss of $1 million or more for APHIS, its business partners, or its stakeholders.

4 Lawsuit for negligence of information whose use and distribution is governed by Trade Secret laws.

5 Grave embarrassment for APHIS, its business partners, or its stakeholders with a reasonable expectation of official censure, outside investigation, or dismissal of senior managers.

(b) Moderate value: If the information were disclosed to unauthorized persons, the likely result would be one or more of the following:

1 Violation of someone's legal right to privacy under the Federal Privacy Act.

2 Litigation for release or misuse of information not governed by the Privacy Act but whose use and distribution is governed by other Federal statutes, contractual agreement, or other mandates.

3 Significant potential threat to APHIS' ability to protect American food supplies and/or support American agriculture and export/import markets.

4 Likely monetary loss of $ 1 00,000 or more (but less than $1 million) for APHIS, its business partners, or its stakeholders.

5 Moderate but manageable embarrassment for APHIS, its business partners, or its stakeholders.

(c) Low value: If the information were disclosed to unauthorized persons, the likely result would be none of the above or other significant impact.

(2) Information Integrity.

(a) High value: If the information in the system became inaccurate or incomplete to a significant degree, the likely result would be one or more of the following:

1 Danger to human life.

2 Grave threat to American food supplies or APHIS' ability to protect American food supplies and/or support American agriculture and export markets.

3 A monetary loss of $1 million or more for APHIS, its business partners, or its stakeholders.

4 Complete or substantial disruption of more than 48 hours.

5 Grave embarrassment for APHIS, its business partners, or its stakeholders with a reasonable expectation of official censure, outside investigation, or dismissal of senior managers.

(b) Moderate value: If the information in the system became inaccurate or incomplete to a significant degree, the likely result would be one or more of the following:

1 Significant potential threat to APHIS' ability to protect American food supplies and/or support American agriculture and export/import markets.

2 Likely monetary loss of $1 00,000 or more (but less than $1 million) for APHIS, its business partners, or its stakeholders.

3 Moderate but manageable embarrassment for APHIS, its business partners, or its stakeholders.

(c) Low value: If the data in the system became inaccurate or incomplete to a significant degree, the likely result would be none of the above or other significant impact.

(3) Information Availability.

(a) High value: If for more than 12 hours the information in the system was unavailable, or the processing and communication of the data was unavailable (excluding the APHIS network), the likely result would be one or more of the following:

1 Danger to human life.

2 Grave threat to American food supplies or APHIS' ability to protect American food supplies and/or support American agriculture and export markets.

3 A monetary loss of $1 million or more for APHIS, its business partners, or its stakeholders.

4 Grave embarrassment for APHIS, its business partners, or its stakeholders with a reasonable expectation of official censure, outside investigation, or dismissal of senior managers.

(b) Moderate value:

1 If for more than 48 hours the information in the system was unavailable, or processing and communication of the data was unavailable (excluding the APHIS network), the likely result would be one or more of the following:

a Grave threat to American food supplies or APHIS' ability to protect American food supplies and/or support American agriculture and export markets.

b A monetary loss of $I million or more for APHIS, its business partners, or its stakeholders.

c Grave embarrassment for APHIS its business partners, or its stakeholders with a reasonable expectation of official censure, outside investigation, or dismissal of senior managers.

2 If for more than 12 hours the information in the system was unavailable, or processing and communication of the data was unavailable (excluding the APHIS network), the likely result would be one or more of the following:

a A monetary loss of $ 1 00,000 or more (but less than $1 million) for APHIS, its business partners, or its stakeholders.

b Moderate but manageable embarrassment for APHIS or for a cooperator/customer.

(c) Low value: If for more than 48 hours the information in the system was unavailable, or processing and communication of the data was unavailable (excluding the APHIS network), the likely result would be none of the above or other significant impact; information availability is not a significant concern.

7. EXCEPTIONS

a. Each APHIS Program/Business Unit must meet the requirements of this Directive. Exceptions that reduce the requirements of this Directive may be approved only in writing by the CIO.

b. Program/Business Units are required to establish ISS safeguards on the basis of identifiable risks. Use of the APHIS risk assessment tool is not mandated for that purpose but is encouraged to promote standardization of ISS measures across the Agency.

8. COMPLIANCE AND SANCTIONS

Functional managers who fail to establish relative values for information resources and use them as the basis for a risk management approach to protect those assets may be held personally accountable for disregarding their fundamental responsibilities. Sanctions include dismissal.

9. INQUIRIES

a. Direct inquiries or requests for change to this Directive to the APHIS ISSPM, 555 South Howes Street, Fort Collins, CO 80521 or call 970-490-7814.

b. This Directive is available at ***www.aphis.usda.gov/library***.

/s/ Michael C. Gregoire
Chief Information Officer